Department of Public Health and Human Services (DPHHS)

Health Insurance Portability and Accountability Act ("HIPAA") Privacy Policy

John Chappuis, Deputy Director

Date: January 3, 2003

Revised Date:

Policy Title:	Physical Security for Protected Health Information		
Policy Number:	014	**Version:**	1.0
Approved By:			
Date Approved:			

Purpose:

This policy addresses the actions necessary to create an environment that protects the security of Protected Health Information ("PHI"). See HIPAA Policy #1, Privacy of Protected Health Information 11-4-02, for definition of PHI.

Policy:

Employees of DPHHS must make reasonable efforts to provide for the security of Protected Health Information.

1. Security of PHI held in electronic medium (includes discs, tapes, computers, etc.)

   a. Each employee is responsible for his/her own uses and disclosures of PHI;

   b. Employees must sign confidentiality statements before obtaining computer access to PHI;

   c. Employees will be granted access to only the level of PHI that is required by their job duties and position description. (For levels of access, see HIPAA Privacy Policy, #13, Employee Access to PHI, December 17, 2002.);

   d. Log-off screens must be used to assure no unauthorized access to computers with PHI. A screen saver with password protection or a complete computer log-off can be used;

   e. Employees may not share passwords or computer access. (See Information Security and database Access Policy 12-15-96.)

   f. Computer screens that can be viewed from common walkways must be repositioned or protected by polarized screen covers.

g. Employees may not access PHI from remote locations using common Internet access;

h. E-mail messaging containing PHI must be conducted over encrypted network lines;

i. E-mail messages containing PHI are not available as public information;

j. When an employee leaves DPHHS, their computer access must be immediately terminated and their password discontinued. Interim access to critical information is the responsibility of the Supervisor;

2. Security of PHI held on paper

a. PHI sent by interagency mail should be sent in routing envelopes that can be differentiated from standard routing mail, such as by using a designated color of envelope. Envelopes containing PHI may be opened by administrative staff, date stamped, returned to the envelope, and then placed in the intended recipient's mailbox in a sealed manner;

b. Only PHI in current use should be exposed on an employee's desktop. All other paper forms of PHI should be covered in file folder when not in use;

c. When the employee is away from the desk for an extended period of time (such as for meal break or to go home for the day) all PHI should be contained in a locked filing cabinet;

d. If at all possible, information should be de-identified before sending on paper to another person;

e. When it is no longer necessary to keep PHI, it must be shredded; and

f. When PHI is to be faxed, the employee will contact the receiver to notify them that a fax is coming, and arrange contact that notifies the sender that the fax has been received. If faxed PHI is received, it should be placed in a designated PHI envelope and placed in the employee's mailbox.

3. Security of PHI in other media, such as oral or telephone

a. Face to face and telephone conversations regarding PHI should be kept to a minimum and should use identifying information as little as possible. For example, a conversation could identify the client with a number rather than a name. In all cases, the conversation must be limited to the minimum information necessary to accomplish the purpose of the communication;

b. Oral conversations about PHI should be conducted in a low voice tone to limit the amount of the conversation that can be overheard by other individuals;

c. Whenever possible, such conversations should be held in a private room or during times when it is less likely that the conversation will be overheard. For example, employees conducting intake or health history interviews should conduct such interviews in private locations or during times when the office is less busy;

d. Sign-in sheets for clinics may be used, but they shall not request the reason for visit; and

e. When receiving telephone calls requesting PHI, the DPHHS employee must validate the identity of the caller before releasing information. In most cases, the request for PHI should be made in writing with a properly signed authorization, or in person with a mechanism to identify the individual requesting the PHI disclosure. In cases where the DPHHS employee may have regular communication with a business associate regarding PHI, the DPHHS employee takes responsibility for validating the identity of the business associate.

Procedure:

I. Each employee will sign a confidentiality statement/physical security checklist when HIPAA training has been completed. The signed form will be maintained in each employee's personnel record.

II. Employees have been assigned a security level and trained for that level of security.

III. Log-off screens are available on all computers. Spot checks will be completed on a random basis to assure they are being used, or that the computer has been logged off on or that the office is locked when the employee is not physically present.

IV. Physical security checks have been completed for positioning of computer screens and inspections will continue on a random basis.

V. Facility e-mail messaging is not on encrypted outside the state system. Do not send e-mail containing PHI to agencies outside the state e-mail system.

VI. Notification to Security Administrators when an employee has terminated employment will be completed by MCDC IT staff at the end of the employee's last work shift or during the IT's next scheduled work shift.

VII. When authorizations for release of PHI are received by mail it will be assumed that the party requesting the information has verified the patient's identity. All signatures on release forms will be checked against patient signature on record at MCDC.

VIII. Picture identification will be requested when former patients appear in person to request information from their medical record. An ID picture of the patient retained in the medical record and will be checked along with the patient's signature releasing any information.

IX. MCDC employees will follow all areas of the above policy.